I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Metadata in Context –An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program

PAULA KIFT & HELEN NISSENBAUM*

CONTENTS

* Paula Kift is a recent graduate of the master's program in Media, Culture and Communication at NYU. Helen Nissenbaum is Director of the Information Law Institute and Professor in the Department of Media, Culture, and Communication at NYU.

I. INTRODUCTION[**]

> A man writes a dozen letters to different people. No person would be permitted to publish a list of the letters written.
>
> —Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy* (1890).

In the aftermath of the Snowden revelations, the National Security Agency (NSA) responded to fears about warrantless domestic surveillance programs by emphasizing that it was collecting only the metadata, and not the content, of communications. When justifying their activities, the NSA offered the following rationale: because data involves content and metadata does not, a reasonable expectation of privacy extends only to the former but not the latter. In other words, the NSA drew a *normative* conclusion about differential treatment of data and metadata based on an *ontological* distinction it claims exists between the two. Our paper challenges this argument. More specifically, we contend that privacy is defined not only by the *types of information* at hand, but also by the *context* in which information is collected. This context has changed dramatically. Defining privacy as contextual integrity we are able, in the first place, to explain why the bulk telephony metadata collection program violated expectations of privacy and, in the second, to evaluate whether the program's purported benefits to national security can be justified – in light of its material costs, on one hand, and its infringements on civil liberties, on the other hand.

The first part of our paper traces the roots of the data/metadata distinction to the library and computer sciences, where metadata is

[**] We are grateful for opportunities to present this work at the Privacy Research Group (PRG) at NYU in April 2015, the European Privacy Law Scholars Conference (PLSC) in October 2015, and the Oxford Internet Institute (OII) in May 2016 where we received invaluable comments. We owe a debt of gratitude to Peter Shane and Dennis Hirsch for organizing the "NSA Bulk Metadata Collection: Evaluating Privacy through the Lens of Contextual Integrity" symposium at The Ohio State University (OSU) Moritz College of Law in November 2016 and to respondents Kiel Brennan-Marquez, Patrick Kelley, Gabe Maldoff, and Omer Tene, for enormously helpful remarks on our paper. Thanks go to Susan Landau for astute commentary. We owe a particular debt to Katherine J. Strandburg and Kiel Brennan-Marquez for generous intellectual guidance throughout the writing process. We acknowledge support from the Digital Trust Foundation (DTF), the Defense Advanced Research Projects Agency (DARPA) and the Hewlett Foundation Cyber Scholars Program.

characterized as data used to describe other data. In the aftermath of the Snowden revelations, however, the courts struggled to characterize metadata in light of precedent. As a result, an assessment of whether the bulk collection of telephony metadata violates a reasonable expectation of privacy seems to have been rooted in three constitutionally relevant dichotomies, namely content vs. non-content data, private records vs. business records held by third parties, and hard-to-obtain information vs. information "in plain view." Our paper traces the genealogy of cases that have influenced these distinctions in order to explain why the judges presiding over the two cases that have challenged the NSA's program thus far – Judge Leon in *Klayman v. Obama* (2013) and Judge Pauley in *ACLU v. Clapper* (2013) – reached opposite conclusions as to whether the bulk telephony metadata collection program violates the Fourth Amendment. Our paper ultimately supports the argument of the *Klayman* court that even if the *nature* of metadata has not changed (and this is debatable), the *circumstances* in which it is collected have. Whether the bulk collection of telephony metadata violates a reasonable expectation of privacy thus requires not only an *ontological* analysis of what metadata "is" but also an assessment of its *normative* significance in light of an evolving social and technological environment.

The second part of the paper develops this normative analysis and demonstrates that the circumstances in which metadata is shared today – be it telephony, internet, location or even biometric "metadata" – are radically different from the circumstances of the cases upon which courts have relied to distinguish metadata from data in the past.[1] These differences primarily manifest themselves in the ability of information subjects to share information *voluntarily*; the ability of the holders of our metadata to *aggregate*, *store*, *combine* and *analyze* that data; and the extent to which we, the data subjects, *assume the risk* of metadata being shared beyond the purpose for which it was originally provided. Significantly, we propose a three-pronged test for evaluating the voluntariness of sharing information with third parties, namely, first, whether a person *knowingly* shares information with a third party, second, whether a person has an *alternative* not to do so, and third, whether that alternative is *reasonable*. Adopting the framework of contextual integrity, the paper then assesses the impact of social and technological changes in the information environment on the *actors*, *attributes* and *transmission*

[1] Most notably Smith v. Maryland, 442 U.S. 735, 741 (1979); *see infra* Section II.B.

principles of relevant information flows to determine whether the NSA's bulk telephony metadata collection program violates the principle of contextual integrity, and hence privacy expectations. In light of contextual values and ends, our evaluation of the program demonstrates that the benefits of the bulk collection of telephony metadata to national security are outweighed by the program's costs, as we take account of both money and manpower, on one hand, and the program's infringements on civil liberties, such as privacy, freedom of speech and association, transparency, due process and the balance of power between the government and its citizens, on the other. The paper concludes that the NSA's justification for its bulk telephony metadata collection program – namely, that metadata is equivalent to non-sensitive data – no longer makes sense. In light of the theory of contextual integrity, it never made any sense to begin with.

II. ONTOLOGICAL ANALYSIS

A. Defining Metadata

Metadata is "data about data," or information used to classify other information.[2] Metadata has played an important role in library and computer sciences because it allows for knowledge management, for example, in the case of books, enabling a useful classification according to such metadata as author, title, date of a publication, as well as publisher, size, number of pages, and genre. In a library catalog, metadata allows patrons to locate books they were expressly seeking or to discover books of potential interest about which they may not have previously known. Beyond books, metadata also plays

---

[2] *See Metadata*, DICTIONARY.COM, http://dictionary.reference.com/browse/metadata [http://perma.cc/NJZ5-K25Q] (defining metadata as "information that is held as a description of stored data"); *Metadata*, OED.COM, http://www.oed.com/view/Entry/117150?redirectedFrom=metadata [http://perma.cc/8HL5-KRR3] (defining metadata as "data that describes and gives information about other data"). The OED also quotes Philip R. Bagley's definition of metadata: "As important as being able to combine data elements to make composite data elements is the ability to associate explicitly with a data element a second data element which represents data 'about' the first data element. This second data element we might term a 'metadata element.' Examples of such metadata elements are: an identifier, a main 'prescriptor' which specifies from what domain the value of the first element must be taken, an access code which limits the conditions under which the first data element can be accessed." PHILIP R. BAGLEY, EXTENSION OF PROGRAMMING LANGUAGE CONCEPTS 26 (1968).

an important role in a myriad of different information searches serving critical organizational functions that we may not typically associate with the term. A Word document, for example, includes metadata such as the file name and author, the time and date of its creation, and the file format and size. Tweets not only consist of 140 signs but also of a host of metadata, including the author's name and biography, the date his account was created, the number of users he is following, and the location and time zone from which his Tweet is sent.[3] What makes metadata so useful is the fact that, generally unlike the contents of a communication, it can be easily read and processed by machines.[4] Indeed, as Cory Doctorow noted in 2001, if everyone were to "create good metadata for the purposes of describing their goods, services and information, it would be a trivial matter to search the Internet for highly qualified, context-sensitive results: a fan could find all the downloadable music in a given genre, a manufacturer could efficiently discover supplies, travelers could easily choose a hotel room for an upcoming trip."[5]

However, the term metadata gained some notoriety in the aftermath of the Snowden revelations as the first set of documents released demonstrated that a classified Foreign Intelligence Surveillance Court (FISC) order had compelled the American telecommunications company Verizon to hand over the telephony metadata of virtually all American subscribers on an ongoing permanent basis.[6] Telephony metadata in this case included "communications routing information, including but not limited to

---

[3] Sarah Perez, *This is What a Tweet Looks Like*, READWRITE (Apr. 19, 2010), http://readwrite.com/2010/04/19/this_is_what_a_tweet_looks_like#awesm=~obCj5KBBrmSTfj [http://perma.cc/69U5-7LA9]. For further examples, see Steven J. Vaughan-Nichols, *Big Data, Metadata, and Traffic Analysis: What the NSA is Really Doing*, IT WORLD (July 26, 2013), http://www.itworld.com/article/2829511/big-data/big-data--metadata--and-traffic-analysis--what-the-nsa-is-really-doing.html [http://perma.cc/C32G-56TU].

[4] Jaron Lanier, *The Meta Question*, THE NATION (July 8, 2015), http://www.thenation.com/article/174776/meta-question [http://perma.cc/RK7R-S8FH].

[5] Cory Doctorow, *Metacrap*, THE WELL (Aug. 26, 2001), http://www.well.com/~doctorow/metacrap.htm [http://perma.cc/PFM6-N2G9]. Doctorow also points to significant limitations to the utility of metadata.

[6] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [http://perma.cc/97GV-7HQP].

session identifying information (e.g., originating and terminating phone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call" but not "the substantive content of any communication."[7] In defending these practices, the NSA asserted that, because it was collecting only the metadata and not the content of communications, its bulk telephony metadata collection program did not raise any privacy concerns.

This argument has now been scrutinized in court: Judge Leon in *Klayman v. Obama* (2013)[8] reached the conclusion that the program violated a reasonable expectation of privacy under the Fourth Amendment, while Judge Pauley in *ACLU v. Clapper* (2013)[9] ruled that it did not. After tracing the genealogy of cases upon which these respective decisions were based, we discovered that in attempting to classify the term metadata in light of precedent, the courts relied on three constitutionally relevant distinctions, namely *non-content v. content data*; *business records held by third parties v. private records*; and *information "in plain view" v. hard-to-obtain information*.[10] Although neither judge argued that the conception of metadata – its ontological status – had changed over time, Judge Pauley maintained that an *ontological* analysis of metadata was sufficient for resolving the case, whereas Judge Leon engaged in a further *normative* analysis of the evolving social and technological environment – an analysis which was ultimately critical to his decision.

---

[7] In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on behalf of MCI Communication Services, Inc. D/B/A Verizon Business Services, No. BR 13-80, at 2-3 (FISA Ct. 2013).

[8] Klayman v. Obama, 957 F. Supp. 2d 1, 39 (D.D.C. 2013).

[9] ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013).

[10] For an excellent technical discussion of the term metadata, see Stephen M. Bellovin, Matt Blaze, Susan Landau & Stephanie K. Pell, *It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law*, HARV. J.L. & TECH. 1 (2016). For a similar discussion in the UK context, see SOPHIE STALLA-BOURDILLON, EVANGELIA PAPADAKI & TIM CHOWN, METADATA, TRAFFIC DATA, SERVICE USE INFORMATION . . . WHAT IS THE DIFFERENCE? DOES THE DIFFERENCE MATTER? AN INTERDISCIPLINARY VIEW FROM THE UK, DATA PROTECTION ON THE MOVE (2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2625181 [http://perma.cc/8KPP-7FU3].

B. Classifying Metadata in the Law

1. Content v. Non-content

The first time the U.S. Supreme Court distinguished between content and non-content was in the context of *Ex parte Jackson* (1878), which questioned whether and the extent to which U.S. authorities could interfere with the mail in order to prevent the circulation of "obscene" materials. The Court concluded that "a distinction is to be made between different kinds of mail matter, – between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined. Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, *except as to their outward form and weight*, as if they were retained by the parties forwarding them in their own domiciles."[11] The Court thus argued that, while police officers should not be able to tear open sealed letters and packages, they should be free to look at the outside appearance and labeling thereof since that information necessarily had to be visible in order to enable them to deliver mail from origin to destination.[12]

In 1928, by contrast, the Court ruled in *Olmstead* that the content of telephone conversations was not analogous to the content of sealed letters. It argued that

> It is plainly within the words of the Amendment to say that the unlawful rifling by a government agent of a sealed letter is a search and seizure of the sender's papers or effects. The letter is a paper, an effect, and in the custody of a Government that forbids carriage except under its protection. The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The Amendment does not forbid

---

[11] Ex parte Jackson, 96 U.S. 727, 733 (1878) (emphasis added).

[12] The protection of the content of sealed letters and packages does not extend to fourth class mail, however. *See* United States v. Riley, 554 F.2d 1282, 1283 (4th Cir. 1977) (arguing that "unlike first class mail, there is no expectation of privacy in the forwarding of fourth class mail . . ." since the petitioner "could have availed himself of the protection afforded by first class postage.").

> what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.[13]

Justice Brandeis, however, disagreed: "the mail is a public service furnished by the Government. The telephone is a public service furnished by its authority. There is, in essence, no difference between the sealed letter and the private telephone message."[14] The content of telephone conversations should consequently enjoy the same legal protection as the content of letters.

The Court revisited this question four decades later in *Katz v. United States* (1967). In *Katz,* the police had attached an electronic listening and recording device to the outside of a telephone booth from which the petitioner was conducting illegal gambling activities. The Court ruled that, although it had "supposed in *Olmstead* that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested. Indeed, we have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements . . . ."[15] According to the *Katz* Court, "no less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[16] But the *Katz* decision was exclusively about the protection of the *contents* of telephone conversations; the *Katz* Court was not in a position to comment on what protections extended to information that was solely *about* the call. Rather, the extent to which the Fourth Amendment protects non-content, as opposed to the content of telephone conversations, was

---

[13] Olmstead v. United States, 277 U.S. 438, 464 (1928).

[14] *Id.* at 475.

[15] Katz v. United States, 389 U.S. 347, 353 (1967).

[16] *Id.* at 352.

decided in the context of *United States v. New York Telephone Company* (1977) and *Smith v. Maryland* (1979).

In *New York Telephone Company*, the Court addressed the question of whether installing and using a pen register device to record the numbers dialed from a phone, falls under the definition of an "intercept" according to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Statute). The Act defined an "intercept" as "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[17] The Court denied that pen registers fall under the definition of the Act "because they do not acquire the 'contents' of communications, as the term is defined by 18 U.S.C. 2510(8)."[18] As the Court explained, "these devices do not hear sound. They disclose only the telephone numbers that have been dialed – a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[19] In distinguishing the register of numbers dialed from the aural, substantive content of the call, the Court thus made an *ontological* distinction between data and metadata on which it furthermore based the *normative* conclusion that "Congress did not view pen registers as posing a threat to privacy of the same dimension as the interception of oral communications . . . ."[20]

The distinction between content and non-content information of telephone conversations was further solidified in *Smith v. Maryland*, a landmark case in Fourth Amendment doctrine. The *Smith* Court addressed the question of whether the warrantless installation and use of a pen register violated a reasonable expectation of privacy under the Fourth Amendment. The petitioner claimed that it did, drawing an analogy to the intercept at issue in *Katz*. However, the *Smith* Court distinguished pen registers "from the listening device employed in *Katz*, for pen registers *do not acquire the contents of communications*"[21] and consequently ruled that pen register

---

[17] *See* 18 U.S.C. 2510(4) (2016).

[18] United States v. New York Telephone Co., 434 U.S. 159, 167 (1977).

[19] *Id.*

[20] *Id.* at 168.

[21] Smith v. Maryland, 442 U.S. 735, 741 (1979) (emphasis added).

information fell outside the ambit of the Fourth Amendment. In response to *Smith v. Maryland*, Congress passed the Pen Register Act, which ensured that pen register information would be granted at least some form of protection under the law, albeit substantially weaker than that granted to the content of communications.[22]

Because the distinction between content and non-content information is primarily drawn in the statutory, not the constitutional context, neither Judge Leon nor Judge Pauley explicitly discusses it in the context of Fourth Amendment law. Both judges do accept, however, that the metadata at issue in the NSA's program is essentially equivalent to the pen register data at issue in *Smith*. As Judge Leon points out, "what metadata *is* has not changed over time. As in *Smith*, the *types* of information at issue in this case are relatively limited: phone numbers dialed, date, time, and the like."[23] Since the case law suggests that pen register data is non-content information, and non-content information is equivalent to non-sensitive information, the telephony metadata collected by the NSA was thus deemed, prima facie, to be non-sensitive information as well.

2. Private records v. Business records held by third parties

Another distinction that significantly influenced the decisions in *ACLU v. Clapper* and *Klayman v. Obama* is that between *private records held by individuals* and *business records held by third parties*. This distinction goes back to a series of cases in the 1950s and

---

[22] *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 295 (5th ed. 2015). The Pen Register Act does not, however, apply to the NSA's bulk telephony metadata collection program because the latter is considered foreign intelligence collection and thus governed by the Foreign Intelligence Surveillance Act (FISA), as amended by Section 215 of the USA PATRIOT Act. *See infra* Section III.B. For a detailed statutory and constitutional analysis of the NSA's bulk telephony metadata collection program, see Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757 (2014).

[23] Klayman v. Obama, 957 F. Supp. 2d 1, 39 (D.D.C. 2013). Quoted in ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y.). At the same time, Judge Leon acknowledges that his statement is not entirely accurate since "the pen register in *Smith* did not tell the government whether calls were completed or the duration of any calls, . . . whereas that information is captured in the NSA's metadata collection." Furthermore, "telephony metadata can reveal the user's location, . . . which in 1979 would have been entirely unnecessary given that landline phones are tethered to buildings." *Klayman*, 957 F. Supp. 2d at 35 (internal citations omitted).

60s in which the Supreme Court decided that the protection of the Fourth Amendment did not extend to incriminating statements made in the presence of undercover police agents.[24] According to the Court, a defendant does not have "a justifiable and constitutionally protected expectation that a person with whom he is conversing will not then or later reveal the conversation to the police."[25] Significantly, the scope of the doctrine of misplaced trust, initially limited to people, was eventually extended to businesses, too. In *United States v. Miller* (1976), the Supreme Court ruled that the petitioner did not have a reasonable expectation of privacy in his bank records because they only contained "information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[26] Referencing *White*, the Court specified that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[27] The majority in *Miller* thus established the consequential third-party doctrine. In *Smith*, too, the Court accepted this reasoning and argued that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[28]

The third-party doctrine significantly influenced Judge Pauley's decision in *ACLU v. Clapper*: "Clear precedent applies because *Smith* held that a subscriber has no legitimate expectation of privacy in telephony metadata created by third parties."[29] Although Judge Leon also acknowledged that the type of data collected by the government in its bulk telephony metadata program was essentially equivalent to

---

[24] *See, e.g.*, United States v. White, 401 U.S. 745, 752-53 (1971); Hoffa v. United States, 385 U.S. 293, 311 (1966); Lewis v. United States, 385 U.S. 206, 212 (1966); Lopez v. United States, 373 U.S. 427, 440 (1963); Lee v. United States, 343 U.S. 747, 757-58 (1952). For a detailed discussion of these cases, see Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 567-569.

[25] *White*, 401 U.S. at 749.

[26] United States v. Miller, 425 U.S. 435, 442 (1976).

[27] *Id.* at 443.

[28] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[29] ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013) (internal citations omitted).

the pen register data at issue in *Smith*,[30] for him this fact was not dispositive. Rather, as we demonstrate in the following section, Judge Leon's decision was influenced by a series of cases that were far more concerned with the changing *nature and circumstances* of government information collection than with the *type* of information collected.

3. Hard-to-obtain information v. Information in plain view

The distinction between hard-to-obtain information and information "in plain view" differs from the previous two in that it does not depend on the *type* of information at hand, but rather on how *easily available* it is. Generally, the courts have decided that petitioners have no reasonable expectation of privacy in information "in plain view" because they assumed the risk that the police would have access to that information.[31] The "plain view doctrine" is based on the idea that officers should not have to turn away from evidence that is right in front of their eyes. However, whether something is "in

[30] *See* Klayman v. Obama, 957 F. Supp. 2d 1, 30 ("The Supreme Court held that Smith had no reasonable expectation of privacy in the numbers dialed from his phone because he voluntarily transmitted them to his phone company . . .").

[31] *See* United States v. Lee, 274 U.S. 559, 563 (1927) (arguing that the use of search lights to examine objects in plain view is permissible under the Fourth Amendment); Ker v. California, 374 U.S. 23, 43 (1963) (arguing that the seizure of a brick of marijuana "did not constitute a search, since the officer merely saw what was placed before him in full view"); Lewis v. United States, 385 U.S. 206, 211 (1966) (arguing that "when, as here, the home is converted into a commercial center to which outsiders are invited for purposes of transacting unlawful business, that business is entitled to no greater sanctity than if it were carried on in a store, a garage, a car, or on the street"); Katz v. United States, 389 U.S. 347, 351 (1967) (arguing that "[w]hat a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection"); Harris v. United States, 390 U.S. 234, 236 (1968) (arguing that "it has long been settled that objects falling in the plain view of an officer who has the right to be in the position to have that view are subject to seizure and may be introduced in evidence"). The "plain view doctrine" was extended by the "open fields doctrine" in that individuals have no reasonable expectation of privacy in the fields that they own. *See* Hester v. United States, 265 U.S. 57, 58-59 (1924) (arguing that the Fourth Amendment does not apply to objects discarded in the open fields even if the land belongs to the petitioner); Oliver v. United States, 466 U.S. 170, 171 (1984) (arguing that "[b]ecause open fields are accessible to the public and the police in ways that a home, office, or commercial structure would not be, and because fences or 'No Trespassing' signs do not effectively bar the public from viewing open fields, the asserted expectation of privacy in open fields is not one that society recognizes as reasonable"). The courts did, however, carve out an exception for a home's so-called curtilage because "the area in question is so intimately tied to the home itself that it should be placed within the home's 'umbrella' of Fourth Amendment protection." United States v. Dunn, 480 U.S. 294, 301 (1987), *quoted in* SOLOVE & SCHWARTZ, *supra* note 22, at 307.

plain view" has become more complicated over time given that police officers increasingly resort to advanced, technologically-enabled surveillance techniques. For instance, in *Florida v. Riley* (1989) the police circled the respondent's property with a helicopter in order to determine, by virtue of two missing roof panels, that the respondent was growing marijuana in a greenhouse adjacent to his home. The majority argued that, "the police, like the public, would have been free to inspect the backyard garden from the street if their view had been unobstructed. They were likewise free to inspect the yard from the vantage point of an aircraft flying in the navigable airspace as this plane was."[32] However, the dissent objected, saying that the question "must be not whether the police were where they had a right to be, but whether public observation of Riley's curtilage was so commonplace that Riley's expectation of privacy in his backyard could not be considered reasonable."[33] A similar question was raised in *Dow Chemical Co. v. United States* (1986) where the Environmental Protection Agency (EPA) used a precision aerial mapping camera to take photographs of a chemical plant. The majority argued that "[t]he mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems."[34] The dissent, on the other hand, objected that this would undermine the court's longstanding "standard that ensured that Fourth Amendment rights would retain their vitality as technology expanded the Government's capacity to commit unsuspected intrusions into private areas and activities."[35] The point at which advanced surveillance techniques become so intrusive that one can no longer speak of information "in plain view" can be determined somewhat more easily when the technologies in question capture information emanating from within the home. For instance, when in *Kyllo v. United States* (2001) the police used a thermal imager to determine whether the suspect was growing marijuana in his home the court argued that the officers obtained information that is "not visible to the naked eye"[36] and thus intruded upon the constitutionally protected space of the

[32] Florida v. Riley, 488 U.S. 445, 449-50 (1989).

[33] *Id.* at 460 (Brennan, J., joined by Marshall, J. and Stevens, J., dissenting).

[34] Dow Chemical Co. v. United States, 476 U.S. 227, 238 (1986).

[35] *Id.* at 240.

[36] Kyllo v. United States, 533 U.S. 27, 29 (2001).

home. In sum, for the above cases, ascertaining whether police officers were collecting information "in plain view" is pertinent to the question whether such collection is subject to Fourth Amendment protection. What constitutes information in "plain view," however, has been complicated by the introduction of new technologies. When, as in *Kyllo*, new technologies are used to capture information emanating from within the home, the Court has generally inclined toward seeing it covered by Fourth Amendment protection.

The Court was confronted with a similar set of questions in cases involving information gathered in public spaces. In *United States v. Knotts* (1983), for example, when the police followed the movements of the defendant by attaching a beeper to a chloroform container he had purchased and placed in his car, the defendant challenged the monitoring on Fourth Amendment grounds. The Supreme Court, however, ruled that "[t]he beeper surveillance amounted principally to following an automobile on public streets and highways. A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements."[37] A beeper, the Court reasoned, did not raise Fourth Amendment concerns in this case because it did not reveal any information "that would not have been visible to the naked eye."[38] The respondent objected that the result of the ruling would be that "twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision."[39] But the Court suggested that these were mere speculations and "if such dragnet-type law enforcement practices as respondent envisions would eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[40] By contrast, in *United States v. Karo*, the Court specified that, while attaching a beeper itself does not raise any Fourth Amendment concerns, it does when the beeper allows the police to track movements within a house.[41] *Karo* was further distinguished

---

[37] United States v. Knotts, 460 U.S. 276, 276 (1983).

[38] *Id.* at 285.

[39] *Id.* at 283 (internal citations omitted).

[40] *Id.* at 284.

[41] "There is no reason in this case to deviate from the general rule that a search of a house should be conducted pursuant to a warrant." United States v. Karo, 468 U.S. 705, 706 (1983).

from *Knotts* on the grounds that, in *Knotts*, the beeper was used to monitor movements in public, while in *Karo* it was used to monitor movements in a private space.[42] In other words, the defendant in *Knotts* assumed the risk of surveillance when travelling on public thoroughfares, whereas in *Karo* the defendant invoked his right against government surveillance within the constitutionally protected space of the home.

At the same time, the court did not categorically rule out that a person could not have a reasonable expectation of privacy in information that is theoretically public. Indeed, in *U.S. Department of Justice v. Reporters Committee for Freedom of Press*, the Supreme Court recognized the defendant's right to privacy in information contained in public rap sheets because "the compilation of *otherwise hard-to-obtain information* alters the privacy interest implicated by the disclosure of that information."[43] The Court effectively created a right to practical obscurity in information contained in public rap sheets.[44] Although the Court has generally been reluctant to extend this right to other contexts,[45] the concept of practical obscurity has resurfaced in other cases, at least implicitly. For example, in *United States v. Jones*, the police engaged in the warrantless GPS monitoring of a suspect's car for a period of 28 days. The majority resolved the case on the basis of the trespass doctrine, arguing that it was the

---

[42] For an early defense of the right to privacy in public, see Helen Nissenbaum, *Toward an Approach to Privacy in Public: Challenges of Information Technology*, 7 ETHICS & BEHAVIOR 207 (1997).

[43] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989) (emphasis added). For a contextual analysis of the impact the digitalization of court records has on privacy concerns, see Amanda Conley, Anupam Datta, Helen Nissenbaum & Divya Sharma, *Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry*, 71 MD. L. REV. 772 (2012).

[44] "Where, as here, the subject of a rap sheet is a private citizen and the information is in the Government's control as a compilation, rather than as a record of what the Government is up to, the privacy interest in maintaining the rap-sheet's 'practical obscurity' is always at its apex while the FOIA-based public interest in disclosure is at its nadir." *U.S. Dep't of Justice*, 489 U.S. at 750 (emphasis added). *See also* Danny Weitzner, *Privacy, Practical Obscurity and the Power of the Semantic Web*, MIT DECENTRALIZED INFO. GRP., http://dig.csail.mit.edu/breadcrumbs/node/125 [https://perma.cc/J9EB-7REN] (defining practical obscurity as "legal doctrine that one may have a privacy interest in the compilation of information (aka a dossier) even though each piece of information composing the dossier is itself publicly available").

[45] *See* Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CAL. L. REV. 1, 21-22 (2013).

attachment of the GPS device to the car that violated the defendant's Fourth Amendment rights. In separate concurrences, Justices Sotomayor and Alito questioned whether the *aggregation* of otherwise public information over time would not raise separate constitutional concerns. Particularly relevant to this article is the connection drawn by Justice Sotomayor between information in plain view (such as a car on public thoroughfares) and information "voluntarily" provided to third parties (referring extensively to information generally classified as metadata): "People disclose the phone numbers they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."[46] Justice Sotomayor ultimately questioned the viability of the third-party doctrine established under *Miller* and *Smith* given the ease with which both metadata and information in plain view, respectively, may be aggregated today.[47]

Judge Pauley, however, refused to attach too much importance to the concurring opinions in *Jones*; after all, the "Supreme Court did not overrule *Smith*."[48] For Judge Leon, on the other hand, the fact that the NSA was collecting telephony metadata in bulk and on an "ongoing daily basis"[49] was dispositive to distinguishing *Klayman v. Obama* from *Smith v. Maryland*.[50] For Judge Leon, the essential question was normative, not ontological. He decided, despite the similarity of the data at hand in *Klayman* and *Smith*, that:

> The question before me is *not* the same question that the Supreme Court confronted in *Smith*. To say the least, 'whether the installation and use of a pen register

---

[46] United States v. Jones, 132 S.Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[47] *Id.* ("I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.").

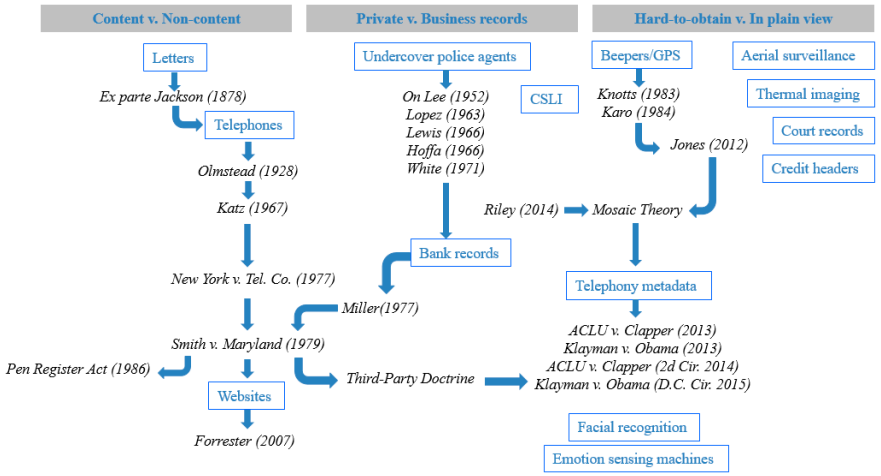
[48] ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013). In support of this argument, see Orin Kerr, *Debate: Metadata and the Fourth Amendment – A Reply to Jennifer Granick*, JUST SEC. (Sept. 23, 2013), https://www.justsecurity.org/1009/debate-metadata-fourth-amendment-reply-jennifer-granick/ [https://perma.cc/32HJ-ZY74].

[49] Greenwald, *supra* note 6.

[50] Klayman v. Obama, 957 F. Supp. 2d 1, 18 (D.D.C. 2013).

> constitutes a 'search' within the meaning of the Fourth Amendment' – under the circumstances addressed and contemplated in that case – is a far cry from the issue in this case. Indeed, the question in this case can more properly be styled as follows: When do present-day circumstances – the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies – become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now.[51]

Figure 1: Genealogy of case law and relevant technologies



[51] *See id.* Laura K. Donohue advances a similar argument in comparing bulk telephony metadata and the pen register data at issue in *Smith*. *See* Donohue, *supra* note 22, at 870-71 ("The extent to which we rely on electronic communications to conduct our daily lives is of a fundamentally different scale and complexity than the situation that existed at the time the Court heard arguments in *Smith*. Resultantly, the extent of information that can be learned about not just individuals, but about neighborhoods, school boards, political parties, Girl Scout troops – indeed, about any social, political, or economic network – simply by placement of a pen register or trap and trace, is far beyond what the Court contemplated in 1979."). *See also* Jennifer Granick, *Debate: Metadata and the Fourth Amendment*, JUST SEC. (Sept. 23, 2013), https://www.justsecurity.org/927/metadata-fourth-amendment/ [https://perma.cc/G2M7-DVG3]. For a general overview of how the evolving social and technological environment affects, or should affect, Fourth Amendment law, see Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614 (2011).

In sum, Judge Pauley emphasizes that the nature of telephony metadata has not changed (telephony metadata are business records, following *Smith*). Judge Leon, by contrast, argues that even if the nature of telephony metadata has not changed (and this is debatable), what *has* changed is the social and technological environment in which metadata is collected. The aggregation of bulk telephony metadata is not comparable to the limited collection of pen register information at issue in *Smith*, echoing *Jones*. In the normative analysis of our paper, we support and further expand on this claim. Based on the theory of contextual integrity, we provide a rigorous account why, even if one accepts that a reasonable line can be drawn between data and metadata, the prima facie assumption that data deserves greater privacy protections than metadata is fundamentally flawed.

III. NORMATIVE ANALYSIS

A. Contextual Integrity

According to the theory of contextual integrity, the appropriateness of a particular information flow depends not only on the *type of information* in question (the *attribute*) but also on the *actors* involved (senders, subjects and recipients of an information type) and the *transmission principles* (constraints on flow). If a practice generates changes in any of these three parameters, a prima facie case exists for claiming that contextual integrity, and hence privacy, has been violated.[52] This prima facie assessment does not necessarily mean, however, that the new practice needs to be abandoned. Indeed, if the new practice better promotes the values, goals and ends of a given context, then contextual integrity allows for and even encourages alterations in information flows.[53]

Material advances in the science and technology of data along with institutional practices have dramatically altered the social and technological environment in which metadata is generated and

---

[52] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 150 (2010).

[53] *Id.* at 182. For a more detailed summary of the theory of contextual integrity, see Helen Nissenbaum, *Respect for Context as a Benchmark for Privacy Online: What it is and isn't*, *in* SOCIAL DIMENSIONS OF PRIVACY 286-88 (Beate Roessler & Dorota Mokrosinska eds., 2015).

collected today. The framework of contextual integrity allows us to assess the impact that these changes have had on information flows. Accordingly, when information subjects no longer share their metadata *voluntarily*, this affects the *transmission principle*. When the recipients of metadata have vastly increased *capabilities* of aggregating, storing, combining and analyzing metadata, this changes the *attribute*. And when we *assume the risk* of surveillance whenever we impart with information, this introduces a wider range of *actors* into the information flow. A careful analysis of these interdependencies also challenges the dichotomies courts have used to distinguish metadata from data, namely: content vs. non-content data, private records vs. business records held by third parties, and hard-to-obtain information vs. information "in plain view."[54] As we argue below, the fact that we no longer share information *voluntarily* undermines the notion that *business records* held by third parties deserve fewer privacy protections than private information held by the data subjects themselves. The fact that metadata is now *aggregated*, *stored*, *combined* and *analyzed* to enable a host of inferences to be drawn undermines the notion that metadata is *non-content* and therefore *non-sensitive* data. The fact that most of our metadata is no longer *hard to obtain* undermines the notion that we should *assume the risk* of surveillance whenever we impart with it.[55] We elaborate on these claims below and explain their significance for our overarching thesis.

---

[54] *See infra* Section II.B.

[55] The last point, in particular, may seem counterintuitive at first, but makes sense when placed in the larger context of a free and open society, in which we should not be forced to assume the risk of surveillance whenever we impart with information; especially when we do not have a reasonable choice to withhold it.

Table 1: Impacts of changes in the social and technical environment on information flows and respective normative implications

	Changes in the social and technical environment	Impact on information flow	Normative implications
Voluntariness	Voluntarily sharing information means knowingly sharing information and having a reasonable alternative not to do so. Even if telephone subscribers knowingly share their metadata with phone companies, they do not have a reasonable alternative not to do so. Telephone subscribers therefore do not share their metadata voluntarily.	This changes the *transmission principle* of the information flow	This undermines the notion that business records should deserve fewer protections than private records.
Capabilities	The recipients of our metadata have vastly increased capabilities of aggregating, storing, combining and analyzing that data.	This changes the *attribute* of the information flow	Metadata can no longer be described as non-content and therefore non-sensitive data because it can be as revealing, if not more revealing, of sensitive information as the content of communications.

	Changes in the social and technical environment	Impact on information flow	Normative implications
Assumption of risk	Previously hard to obtain metadata has become easily accessible so that we effectively assume the risk of surveillance whenever we impart with the information.	This introduces a vastly increased range of *actors* into previously limited information flows	In a free and open society, communications metadata should deserve stronger legal protections as to not be as readily available to the police as it currently is.

1. Voluntariness

The question of voluntariness emerged in the early days of the third-party doctrine. We recall that, in *United States v. Miller*, the Court rejected the idea that the respondent enjoyed Fourth Amendment protection in his bank records because "all of the documents obtained, including financial statements and deposit slips, contain *only information voluntarily conveyed to the banks* and exposed to their employees in the ordinary course of business."[56] Along the same lines, in *Smith v. Maryland*, the majority suggested that "[w]hen he used his phone, petitioner *voluntarily* conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."[57] However, the notion that the petitioners "voluntarily" handed over their data to the phone company and bank, respectively, was already contested at the time the cases were argued.[58] In *Miller*, for example, Justice Brennan noted that "the disclosure by individuals or business firms of their financial affairs to

[56] United States v. Miller, 425 U.S. 435, 442 (1976) (emphasis added).

[57] Smith v. Maryland, 442 U.S. 735, 744 (1979) (emphasis added).

[58] For an early criticism in the academic literature, see John S. Applegate & Amy Applegate, *Pen Registers after Smith v. Maryland*, 15 HARV. CIV. RIGHTS - CIV. LIBERTIES L. REV. 753, 765 (1980) ("The argument advanced by the Court that telephone users know that records will be made of toll calls and thus have no expectation of privacy is unconvincing.").

a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[59]

Compare these two with cases involving cell-site location information (CSLI): Theoretically, CSLI is non-content information "in plain view" voluntarily conveyed to third parties, and some courts have indeed supported that claim. For instance, according to the United States Court of Appeals for the Fifth Circuit, "[b]ecause a cell phone user makes a choice to get a phone, to select a particular service provider, and to make a call, and because he knows that the call conveys cell site information, the provider retains this information, and the provider will turn it over to the police if they have a court order, he *voluntarily* conveys his cell site data each time he makes a call."[60] But this distorts the original information flow. A cell phone user (the sender and information subject) conveys his cell site data (the attribute) "voluntarily" (the transmission principle) only to the service provider (the intended recipient). Once the information is passed to the police, the cell phone user has not "voluntarily" provided anything at all. Neither the recipient nor the transmission principle of the information flow are the same anymore.

A further complication in the CSLI cases arises from the fact that most cell phone users do not even provide CSLI *knowingly*: "When a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all. And a caller most certainly does not voluntarily provide the registration information that the phone automatically sends to the phone company every seven seconds whenever the phone is on, without notice to or control by the user."[61] This sentiment was later echoed by the Eleventh Circuit and most

---

[59] *Miller*, 425 U.S. at 451 (Brennan, J., dissenting) (quoting Burrows v. Superior Court, 13 Cal. 3d 238, 247 (1974)).

[60] In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 614 (5th Cir. 2013) (emphasis added).

[61] Brief for Elec. Frontier Found. et al. at 21, as Amici Curiae Supporting Affirmance, In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304 (3rd Cir. 2010), https://www.eff.org/files/filenode/celltracking/filed_cell_tracking_brief.pdf [https://perma.cc/Z2G7-4UYX]; *see also* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 684 (2011).

recently by the Fourth Circuit.[62] The U.S. District Court, Southern District of Texas, further explains:

> Unlike the bank records in *Miller* or the phone numbers dialed in *Smith*, cell site data is neither tangible nor visible to a cell phone user. When a user turns on the phone and makes a call, she is not required to enter her own zip code, area code, or other location identifier. None of the digits pressed reveal her own location. Cell site data is generated automatically by the network, conveyed to the provider not by human hands, but by invisible radio signal. Thus, unlike in *Miller* or *Smith*, where the information at issue was unquestionably conveyed by the defendant to a third party, a cell phone user may well have no reason to suspect that her location was exposed to anyone. The assumption of risk theory espoused by *Miller* and *Smith* necessarily entails a knowing or voluntary act of disclosure; the Government has cited no case (and the court has found none) where unknowing, inadvertent disclosure of information by a defendant thereby precluded Fourth Amendment protection of that information.[63]

It is worth noting the connection between these insights and traditional philosophical positions on (moral) responsibility, which require at the very minimum that actors are morally responsible for their actions insofar as they have been performed freely and knowingly.[64] This account forms the basis of informed consent and the foundation for legal concepts surrounding liability. In our view, the limited understanding most of us have of digitally intermediated communication calls into question whether individuals using mobile phones, for the most part, are disclosing CSLI (and other metadata) voluntarily, let alone knowingly.

---

[62] United States v. Davis, No. 12-12928, at 22 (11th Cir. 2014); United States v. Graham, 796 F.3d 332, 353 (4th Cir. 2015).

[63] In re Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 844 (2010), *vacated*, 724 F.3d 600 (5th Cir. 2013).

[64] *See, e.g.*, Joel Feinberg, *Sua Culpa*, *in* DEBORAH G. JOHNSON & JOHN W. SNAPPER, ETHICAL ISSUES IN THE USE OF COMPUTERS (1985); JOHN MARTIN FISCHER & MARK RAVIZZA, S.J., RESPONSIBILITY AND CONTROL: A THEORY OF MORAL RESPONSIBILITY (1st ed. 1998).

But even if the defendants in *Miller* and *Smith* voluntarily *and* knowingly conveyed information to a third party, they conveyed that information to a business for a particular purpose, and not to the police for the purpose of a criminal investigation. This is one of the reasons why transforming personal records into business records should not diminish but rather reinforce privacy expectations. When personal information is provided to create a business record, the reasonable expectation is precisely that that information will only be used for a *business* purpose. For this reason, we find the notion that there is no reasonable expectation of privacy in information held in business records to be fundamentally flawed.[65]

Several states have already rejected the third-party doctrine on this basis.[66] For instance, in the context of a CSLI case in New Jersey, the state's supreme court pointed out that "an individual's privacy interests under New Jersey law does not turn on whether he or she is required to disclose information to third-party providers to obtain service. Just as customers must disclose details about their personal finances to the bank that manages their checking accounts, cell-phone users have no choice but to reveal certain information to their cellular provider. That is not a voluntary disclosure in a typical sense; it can only be avoided at the price of not using a cell phone."[67]

Similarly, the Supreme Court ruled in *Ferguson v. City of Charleston* that the police could not conduct warrantless and nonconsensual drug tests on urine samples provided by pregnant

---

[65] *See also* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 654 (2015) (arguing that entrusting so-called "information fiduciaries" with personal information "carries an implicit limitation on use: specifically, an implied covenant to avoid using sensitive information in ways that harm the sharing party").

[66] *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373 (2005), *quoted in* SOLOVE & SCHWARTZ, *supra* note 22, at 296.

[67] New Jersey v. Earls, 70 A.3d 630, 641 (N.J. 2013). A similar argument has been made with regard to telephony and Internet metadata collection: "Even if U.S. citizens wanted to opt out of having this information collected, it would be virtually impossible to do so. There have, for instance, been advances in encryption. But these technologies all revolve around content – not metadata. Although some technologies are focused on metadata, these are not sufficiently advanced to allow for real-time communication. The only option is therefore not to use a telephone. The cost of doing so, however, would lean towards divesting oneself of a role in the modern world – impacting one's social relationships, employment, and ability to conduct financial and personal affairs." Donohue, *supra* note 22, at 874.

women to a state hospital for the purpose of obstetric tests. According to the majority, the urine tests were "indisputably searches within the meaning of the Fourth Amendment" and that "none of the women searched provided either probable cause to believe that they were using cocaine, or even the basis for a reasonable suspicion of such use."[68] Moreover, under the two-pronged *Katz* test, the majority ruled that "the reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests *will not be shared with nonmedical personnel without her consent*."[69] The latter point earned a scathing response from the dissent. In reference to the cases involving the use of undercover police agents, Justice Scalia acknowledges that "abuse of trust is surely a sneaky and ungentlemanly thing, and perhaps there should be (as there are) laws against such conduct by the government."[70] At the same time, Scalia found that, until *Ferguson*, the majority has "*never* held – or even suggested – that material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain. Without so much as discussing the point, the Court today opens a hole in our Fourth Amendment jurisprudence, the size and shape of which is entirely indeterminate."[71] Justice Scalia is correct in that the decision in *Ferguson* "represents a significant departure from the third-party doctrine. Indeed, is urine voluntarily turned over to a hospital really any different from tax documents turned over to a bank or metadata transmitted to the phone company?"[72] Most important, however, is that *Ferguson* further undermines the third-party doctrine's notion of "voluntariness." If the warrantless search of urine tests provided to a hospital for the purpose of obstetric test were constitutional, it could only be avoided at the price of not making use of obstetric tests at all.

---

[68] Ferguson v. City of Charleston, 532 U.S. 67, 76 (2001).

[69] *Id.* at 78 (emphasis added).

[70] *Id.* at 94 (Scalia, J., dissenting).

[71] *Id.* at 95.

[72] Alexander Galicki, *The End of Smith v. Maryland?: The NSA's Bulk Telephony Metadata Program and the Fourth Amendment in the Cyber Age*, 52 AM. CRIM. L. REV. 375, 397 (2015). This interpretation of *Ferguson. v. Charleston* was recently confirmed by the U.S. Court of Appeals for the Fourth Circuit: "That the government acquired Appellants' private information through an inspection of third-party records cannot dispose of their Fourth Amendment claims." United States v. Graham, 796 F.3d 332, 352 (4th Cir. 2015).

A Three-Pronged Test

In line with these conclusions, we suggest that courts should transform their assessment of "voluntariness" into a three-pronged test: first, whether a person *knowingly* shared information with a third party; second, whether a person had an *alternative* not to do so; and third, whether that alternative was *reasonable*. If the answer is "yes" to all questions (as is the case with misplaced trust in undercover police agents), then a person should not have a reasonable expectation of privacy for the revealed information. If the answer is "no" to all questions (as is the case with CSLI) or "yes" to the first two questions but "no" to the third (as is the case in *Ferguson v. Charleston*), then a person should retain a reasonable expectation of privacy for the information revealed.

2. Capabilities

The more limited collection of pen register data at issue in *Smith v. Maryland* in 1979 is not comparable to the massive aggregation of telephony metadata at issue in the NSA's 2013 bulk telephony metadata collection program. In *Smith,* the police had ordered the telephone company to register the numbers dialed from the phone of a single person in the context of a specific, temporally limited police investigation. By contrast, according to the Snowden documents, the NSA collected the telephony metadata of virtually all American subscribers in the context of an ongoing national security operation, regardless of whether they were suspected of any criminal behavior.[73] Furthermore, as the *Klayman* court points out, the NSA program involved "the creation and maintenance of a historical database containing *five years*' worth of data"[74] and, at the time of the ruling,

---

[73] Subsequent accounts questioned whether the NSA was actually collecting that much metadata. *See* Siobhan Gorman, *NSA Collects 20% or Less of U.S. Call Data*, WALL ST. J. (Feb. 7, 2014), http://www.wsj.com/articles/SB10001424052702304680904579368831632834004 [https://perma.cc/8EVH-P2ZA]. However, as several commentators point out in the article, this does not make the program any less concerning. First, the NSA still collected millions of phone records on a questionable legal basis; second, even if it was not successful, it still aspired to collect the vast majority of phone records; and third, the fact that the NSA may not actually have collected all the phone records undermines their justification for having the program in the first place, namely, to "have the entire haystack" for "finding the needle."

[74] Klayman v. Obama, 957 F. Supp. 2d 1, 19 (D.D.C. 2013) (emphasis added).

there was no planned end of the bulk telephony metadata collection program either. According to the United States Court of Appeals for the Second Circuit, which reviewed Judge Pauley's decision in *ACLU v. Clapper* and ultimately overruled it, "[s]uch expansive development of government repositories of formerly private records would be an unprecedented contraction of the privacy expectations of all Americans."[75]

Table 2: A contextual comparison of Smith v. Maryland and the NSA's bulk telephony metadata collection program

	Smith v. Maryland (1979)	Bulk Telephony Metadata Collection Program (2013)
Context	Single police investigation	Ongoing national security investigation
Senders	Single American telephone subscriber suspected of criminal activity	All American telephone subscribers, regardless of whether they are suspected of any criminal activity
Subject	Various	Various
Attribute	Numbers dialed on a phone	Numbers that placed and received the call, the data, time, and duration of the call, other session-identifying information (for example, International Mobile Subscriber Identity number, International Mobile Station Equipment Identity number, etc.), trunk identifier, and any telephone calling card number
Transmission principle	None; then ECPA (1986)	Section 215 of the USA PATRIOT Act (2001)

Furthermore, technological innovations facilitate the storage of a much greater amount and variety of data.[76] These innovations go both ways: not only can the NSA store significantly more data, but individuals can also create and maintain much larger databases of personal information themselves. For instance, as the Supreme Court recognized in *Riley v. California* (2014), cell phones have effectively

[75] ACLU v. Clapper, 785 F.3d 787, 818 (2d Cir. 2015).

[76] *See* Declaration of Professor Edward W. Felten at 23, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-3994).

become "minicomputers." "The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos."[77] The amount of information that can be gleaned from a single device is unprecedented. Cell phones contain not only call data, but also Internet browsing history and location data, all of which, according to precedent, are considered non-content information held by third parties and information "in plain view," respectively, and thus equally undeserving of the protection of the Fourth Amendment on a purely ontological basis.[78]

One could object that the NSA did not actually collect all this information in its bulk telephony metadata collection program; however, as Judge Leon points out in several footnotes to his ruling, the exact scope of the telephony metadata program remains unclear. For instance, Judge Leon could not determine "whether 'telephony metadata' and 'comprehensive communications routing information' include data relating to text messages. If it does, then in 2012, the Government collected an additional *six billion* communications *each day* (69,635 *each second*)."[79] Furthermore, despite the fact that later FISC orders explicitly prohibited the production of CSLI, "not all FISC orders have been made public, and I have no idea how location data has been handled in the past."[80] But, even if the NSA did not collect these kinds of information as part of its bulk telephony metadata collection program – and the courts were therefore not in a position to define them – it is important to keep in mind that they *could* plausibly be defined as metadata in the future,[81] which has serious privacy

---

[77] Riley v. California, 134 S.Ct. 2473, 2489 (2014).

[78] *See id.* (pointing out that "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet"). *See also* SUSAN LANDAU, SURVEILLANCE OR SECURITY?: THE RISKS POSED BY NEW WIRETAPPING TECHNOLOGIES 99 (2011) (describing transactional data, i.e., metadata, as the "new gold" of wiretapping).

[79] *See* Klayman, 957 F. Supp. 2d at 35 (internal citations omitted).

[80] *Id.* at 36.

[81] The D.C. Court of Appeals already predicted this in reviewing *ACLU v. Clapper*: "If the government is correct, it could use §215 to collect and store in bulk any other existing metadata available anywhere in the private sector, including metadata associated with financial records, medical records, and electronic communications (including e-mail and

implications if judges continue to rely on an ontological rather than a contextual analysis of metadata collection.[82]

In the context of Internet communications, that determination has already been made: In *United States v. Forrester*, the court ruled that Internet users have no reasonable expectation of privacy in e-mail headers and IP addresses because they should know that Internet service providers (ISPs) necessarily have access to that information in order to provide their services.[83] (We note that according to our three-pronged test, however, this reasoning fails the voluntariness requirement.) Significantly, the court also found that the *type* of information at hand was indistinguishable from the pen register information at issue in *Smith*: "e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers."[84] Based on a purely ontological analysis, addressing information is metadata and therefore non-sensitive data.

Finally, as noted earlier, computers can easily *analyze* metadata because it is structured and predictable. This distinguishes it from the content of communications which computers still struggle to

---

social media information), relating to all Americans." ACLU v. Clapper, 785 F.3d 787, 818 (2d Cir. 2015).

[82] As a thought experiment, consider recent developments in the field of biometrics: FaceIt, a facial recognition software, "can pick someone's face out of a crowd, extract the face from the rest of the scene and compare it to a database of stored images." *See* Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOW STUFF WORKS, http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition1.htm [https://perma.cc/Y37A-HGJ3]. It can differentiate one face from another based on so-called nodal points, such as the distance between the eyes, width of the nose, depth of the eye sockets, the shape of the cheekbones, the length of the jaw line, etc. One could argue that the nodal points constitute the metadata of the face, whereas the identity of the person constitutes the content. Emotion sensing machines such as Affdex function in a similar manner: "The software scans for a face, if there are multiple faces, it isolates each one. It then identifies the face's main regions – mouth, nose, eyes, eyebrows – and it ascribes points to each, rendering the features in simple geometries." *See* Raffi Khatchadourian, *We Know How You Feel*, THE NEW YORKER (Jan. 1, 2015), http://www.newyorker.com/magazine/2015/01/19/know-feel [https://perma.cc/KM84-HF5Q]. The identifiers, again, could reasonably be described as the metadata of the face, whereas the emotions people are experiencing would be considered content. Since the latter can automatically be derived from the former, however, we imagine that people would demand an equal level of privacy protection for both.

[83] United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007).

[84] *Id.* Meanwhile, scholars have demonstrated that email headers do, in fact, contain content information and are thus not equivalent to addressing information on physical mail. *See* Bellovin et al., *supra* note 10.

comprehend.[85] An analysis of the aggregated metadata then not only enables the NSA to infer patterns about social relations and associations,[86] but also about political and religious beliefs[87] and even sensitive medical conditions.[88] This is one of the big ironies behind the idea that metadata can be distinguished from data on the basis that it does not reveal anything about the underlying "content" of communications. Indeed, as we outlined in Section II.A of our paper, the entire purpose of metadata in library and computer sciences is to classify and thus reveal essential aspects about the data that it describes.[89]

What the foregoing analysis attempted to demonstrate is that as capabilities in aggregation, storage, combination and analysis of metadata increase, so does the amount of information that can be gleaned from collecting it. Although we may reasonably expect that a cell phone service provider collects the numbers dialed from a phone, generally, we do not expect the provider to simultaneously learn about our daily whereabouts, our friends and family, our professional associations, and our religious denomination. Therefore, as the social and technological environment changes, so does the meaning or significance of the *attributes* in an information flow. This is an

---

[85] Especially spoken communication, given different rhythms and intonations of speech, as well as accents. *See* Felten Declaration, *supra* note 76, ¶ 21.

[86] For a visual representation of what the analysis of aggregated metadata might look like, see *Immersion Project*, MIT MEDIA LAB, https://immersion.media.mit.edu [https://perma.cc/2FNJ-Y4ZJ].

[87] *See* Felten Declaration, *supra* note 76, ¶ 46. Since the bulk collection of metadata enables law enforcement to identify networks and relationships, it also raises First Amendment, and in particular freedom of association, concerns. *See* Katherine J. Strandburg, *Membership Lists, Metadata, and Freedom of Association's Specificity Requirement*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 327 (2014).

[88] Jonathan Mayer et al., *Evaluating the Privacy Properties of Telephone Metadata*, 113 PROC. NAT'L ACAD. SCI. 5536 (2016), http://www.pnas.org/content/113/20/5536.full.pdf [https://perma.cc/644N-EBH]. Interestingly, a number of legal scholars already made this argument in the aftermath of *Smith v. Maryland*. *See* Applegate & Applegate, *supra* note 58, at 766. But of course, the revelatory power of metadata today is even greater.

[89] Sometimes metadata can be even more revealing than the content of communications: "Significant social analysis can also be conducted on the data. Sophisticated algorithms, for instance, can be applied to pen register information to ascertain where the important nodes are in a network. Alliances, friendships, and predilections can be uncovered by studying patterns in behavior. And unlike raw content, the type of information that can be gleaned is ordered – making it in some ways even more useful than the content itself." *See* Donohue, *supra* note 22, at 871.

important point because it fundamentally undermines one of the most important assumptions underlying the NSA's justifications for the bulk telephony metadata program, namely that metadata is inherently non-sensitive data. From the perspective of the theory of contextual integrity, this assumption never made any sense to begin with: no information type is inherently sensitive or not. Rather, the privacy interest associated with a type of information can only be determined in light of an evaluation that takes into consideration all contextual parameters, including the senders, subjects and recipients as well as transmission principles governing the information flow.

3. Assumption of risk

Often, we do not share metadata voluntarily. Furthermore, technological innovations in aggregation, storage, combination and analysis increase the ability of those with whom we share our data to extract useful information from that data. But beyond that, changes in the social, technological and legal environment have made previously hard to obtain metadata easily accessible so that we effectively assume the risk of surveillance whenever we communicate. The extension of the doctrine of misplaced trust from people to businesses is a telling case. Of course, nobody can protect us against sharing personal information with a friend who turns out to be not that great of a friend or, in particular instances, an undercover police agent.[90] When we share intimate information with others we indeed assume the risk that those with whom we share our data will be untrustworthy. However, the nature of the information sharing changes radically when the recipients of an information flow are no longer people but businesses, e.g. banks, telephone and web service providers, and hospitals. The question here is no longer about the terms of a friendship but the terms of a transaction. Of course, the Supreme Court ruled in *United States v. Miller* that

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and

[90] In Germany, by contrast, undercover policing "entails a warrant procedure, a showing of need, and statutory limits on the crimes that the government may target in this way," out of a historical concern for human dignity. *See* Jacqueline E. Ross, *The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany*, 55 AM. J. COMP. L. 493, 562 (2007), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=909010 [https://perma.cc/2BPY-S9V8]. *See also* SOLOVE & SCHWARTZ, *supra* note 22, at 287.

> conveyed by him to Government authorities, *even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed*.[91]

However, in order to support this claim, the Court exclusively referenced cases involving undercover police agents, despite the fact that a relationship between people is governed by a completely different set of transmission principles than a relationship between a person and a bank.[92] Justice Brennan readily dismissed this argument in dissent, quoting representatives from several banks according to whom "a bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes."[93] The dissent in *Smith v. Maryland* echoed similar concerns: "Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[94] Furthermore:

---

[91] United States v. Miller, 425 U.S. 435, 443 (1976) (emphasis added). What makes the *Miller* case particularly contentious is that that "the bank did not just happen to be holding the records the government sought. Instead, the Bank Secrecy Act required (and continues to require) banks to maintain a copy of every customer check and deposit for six years or longer. The government thus compelled the bank to store the information, and then sought the information from the bank on the basis that since the bank held the data, there could not be any reasonable expectation of privacy and the Fourth Amendment therefore did not apply." Fred H. Cate & Beth E. Cate, *The Supreme Court and Information Privacy*, 2 INT'L. DATA PRIVACY L. 255, 263 (2012), https://academic.oup.com/idpl/article/2/4/255/676934/The-Supreme-Court-and-information-privacy [https://perma.cc/FA7K-BXLA].

[92] This discrepancy has been pointed out before: "*Miller* based this 'assumption of risk' argument on two informer cases, *United States v. White* and *Hoffa v. United States*. But to name these cases suggests the distinction: one expects a human being to evaluate, digest, recall, and perhaps repeat information; a bank merely performs and registers a transaction." Applegate & Applegate, *supra* note 58, at 756; *see also* Brennan-Marquez, *supra* note 65.

[93] *Miller*, 425 U.S. at 449 (1976) (Brennan, J., dissenting).

[94] Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting). The same argument was made in the context of mail covers: "[A] reasonable person expects (1) that the information contained in the return address will only be used for mail purposes, and (2) that it will be utilized in only a mechanical fashion without any records being kept. The recording and disclosure to non-postal authorities for non-postal purposes that results from a mail cover extends far beyond these narrow bounds." United States v. Choate, 422 F. Supp. 261, 270 (C.D. Cal. 1976).

> At least in the third-party consensual surveillance cases, which first incorporated risk analysis into Fourth Amendment doctrine, the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications. By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance.[95]

At present, of course, sharing personal information and the associated metadata with third parties has become an even greater personal and professional necessity. A 2013 longitudinal study of American youth revealed that young adults communicate about as much via digital media such as email and social networks as they communicate face-to-face.[96] Cell phones, as Judge Leon points out in *Klayman v. Obama*, have become ubiquitous:

> Count the phones at the bus stop, in a restaurant, or around the table at a work meeting or any given occasion. Thirty-four years ago, *none* of these phones would have been there. Thirty-four years ago, city streets were lined with pay phones. Thirty-four years ago, when people wanted to send 'text messages,' they wrote letters and attached postage stamps.[97]

The pervasive use of electronic devices, often connected to the Internet, generates an overwhelming quantity of metadata, which would all remain unprotected were we to assume that any disclosure to a third party exposes us to further risks of surveillance. Most importantly, as Judge Leon points out in direct reference to *U.S. Dep't*

---

[95] *Smith*, 442 U.S. at 749-50 (1979) (Marshall, J., dissenting). A similar argument was made in the case preceding *Smith v. Maryland*: "Even if the majority's analogy to *Miller* is valid, (and I do not agree) and Smith should have expected that the telephone company could itself monitor his phone for billing purposes, to improve service to its customers, or to verify complaints, Smith nevertheless had a reasonable expectation that the telephone company would not, without the safeguards of appropriate legal process, act for the government in collecting information relevant to a criminal prosecution." Smith v. Maryland, 389 A.2d 858, 872-73 (C.A. Md. 1978) (Cole, J., dissenting).

[96] Jon D. Miller, *Social Capital: Networking in Generation X*, 2 Generation X Rep. 2, 6 (2013), http://lsay.org/GenX_Vol2Iss2.pdf [https://perma.cc/KYF3-WU5T].

[97] Klayman v. Obama, 957 F. Supp. 2d 1, 35 (D.D.C. 2013).

of Justice v. Reporters Comm. for Freedom of Press, "[i]t's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence operation with the Government."[98] Thus, the NSA program essentially introduced a completely different set of recipients into the original information flow between telephone users and service providers, thereby violating contextual integrity and hence also the privacy expectations of the customers so affected.

Apart from *U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press* and *Jones*, cases emerging in the context of finance have also supported the proposition that individuals should not be forced to assume the risk of surveillance whenever they disclose information, particularly if the information in question was previously hard to obtain. A case in point is the dispute between the Federal Trade Commission (FTC) and the credit bureaus when Congress passed the Gramm-Leach-Bliley Act (GLBA), which:

> [R]equired financial institutions to provide notice to consumers prior to transmitting covered information to others, and to permit them to opt out (subject to certain exceptions). This meant that credit header information, which previously had been freely sold (for such purposes as target marketing), was now subject to GLBA requirements.[99]

While TransUnion and the Individual Reference Services Group (IRSG) had assumed a narrow definition of financial information, which would be regulated by the GLBA, it turned out that the definition of non-public personal information (NPI) Congress assumed was wider-ranging, including "any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information."[100] According to the court this meant that Congress had "provided for especially broad privacy protections for all information contained in these lists of consumers

---

[98] *Id.* at 33.

[99] NISSENBAUM, *supra* note 52, at 154.

[100] 15 U.S.C. § 6809 (1999).

that is derived using nonpublic personal information. *This is so even where the information is otherwise publicly available*: the information is still protected, as long as it was derived using nonpublic personal information."[101] The court thus recognized a right to privacy in the information, despite the fact that it was available in public. In our view this can be attributed both to an unacknowledged shift in transmission principle – when information is provided by commercial credit bureaus instead of public channels – and to the violation of a reasonable expectation of privacy in public information – when it is compiled and used out of context.

B. Evaluation

The NSA's bulk telephony metadata collection program has introduced changes in the actors, attributes and transmission principles of the information flows in a national security context and therefore constitutes a prima facie violation of the principle of contextual integrity. But the analysis does not end here. While the theory presumptively favors protecting the integrity of entrenched informational norms – more simply, the status quo – it also allows for information environments to evolve "if new practices are demonstrably more effective at achieving contextual values, ends, and purposes or the equivalent."[102] A contextual analysis of the NSA's bulk telephony metadata program therefore requires an evaluation of the moral and political factors affected by the program and whether the benefits of its disruptive information flows outweigh potential costs as a function of its impact on contextually specific goals and ends.[103]

The *context* in question is that of national security. Following the traumatic events of September 11, 2001, the prevention of any further terrorist attacks and the concomitant loss of American lives on American soil became a paramount goal of U.S. homeland security. Critics have pointed out, however, that the intelligence community was hampered not predominantly because of insufficient information *collection* but because of failures in information *sharing* practices between intelligence and law enforcement agencies, such as the NSA

---

[101] Individual Reference Services Group, Inc. v. FTC, 145 F. Supp. 2d 6, 27 (D.D.C. 2001) (emphasis added).

[102] NISSENBAUM, *supra* note 52, at 180.

[103] *Id.* at 182.

and FBI – information they already had thanks to conventional law enforcement techniques.[104] Nevertheless, pressed to answer for the terrible events of 9/11, the intelligence community radically expanded the scope of its information collection efforts.[105]

Even the remote possibility that the collect-it-all approach might forestall terrorism may explain why the intelligence community interpreted the FISA business records provision as it did – that is, to justify the bulk telephony metadata collection program. The business records provision states that "the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items)" provided that "the tangible things sought are *relevant* to an authorized investigation."[106] Given that terrorists could be hiding behind any number of telecommunications devices in the United States, the government relied on this language to argue "that *all* telephone calls in the United States, including those of a wholly local nature, are 'relevant' to foreign intelligence investigations."[107] As several commentators have since pointed out, this stretches the relevance standard beyond recognition as "any data might be 'relevant' to an investigation eventually, if by 'eventually' you mean 'sometime before the end of time.'"[108]

Theoretically these measures could, however, be justified in light of contextual integrity if they ultimately achieve the goal of national security more effectively than past measures, namely in preventing

---

[104] *See* PETER BERGEN ET AL., NEW AM. FOUND., DO NSA'S BULK SURVEILLANCE PROGRAMS STOP TERRORISTS? (2014), https://www.newamerica.org/downloads/IS_NSA_surveillance.pdf [https://perma.cc/9J7L-VWRK]; *see generally* Mattathias Schwartz, *The Whole Haystack*, THE NEW YORKER (Jan. 26, 2015), http://www.newyorker.com/magazine/2015/01/26/whole-haystack [https://perma.cc/Q543-ZSAH].

[105] *See* GARRETT M. GRAFF, THE THREAT MATRIX: THE FBI AT WAR 391-430 (2011).

[106] *See* Foreign Intelligence Surveillance Act of 1978, § 501, 50 U.S.C. § 1861 (2016) (emphasis added).

[107] *See* Donohue, *supra* note 22, at 836-37 (2014).

[108] Jennifer Stisa Granick & Christopher Jon Sprigman, *The Criminal N.S.A.*, N.Y. TIMES (June 27, 2013), http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html?_r=0 [https://perma.cc/ZR99-PGCJ].

future terrorist attacks. As if responding to this requirement, U.S. government and intelligence representatives repeatedly claimed that the bulk telephony metadata collection program contributed to thwarting over 50 different terrorist attacks.[109] These claims, however, were challenged in a report of the Privacy and Civil Liberties Oversight Board (PCLOB), which was tasked with evaluating the surveillance programs made public through the Snowden revelations. The Board was unable to identify "a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation."[110] The only case in which the bulk collection of telephony metadata played a significant role in the containment of terrorist activity was in the arrest of Basaaly Moalin, a Somali-born citizen, who was convicted of sending $8,500 to the Shabaab.[111] Even in this case, the PCLOB cautioned that "the suspect was not involved in planning a terrorist attack and there is reason to believe that the FBI may have discovered him without the contribution of the NSA's program."[112]

Costs associated with the bulk collection of telephony metadata have been significant. It is difficult for civilians to assess financial costs precisely because much of the relevant information remains classified and we can only assume that the program forms part of the "massive increases in homeland security expenditures that have taken place since 9/11 – increases that total well over $1 trillion."[113] Even if total costs have not increased, however, allocating resources to

[109] *See* BERGEN ET AL., *supra* note 104; Justin Elliott & Theodoric Meyer, *Claim on 'Attacks Thwarted' by NSA Spreads Despite Lack of Evidence*, PROPUBLICA (Oct. 23, 2013), http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence [https://perma.cc/T5VD-3J6E]; Cindy Cohn & Dia Kayyali, *The Top 5 Claims that Defenders of the NSA have to Stop Making to Remain Credible*, ELECTRONIC FRONTIER FOUND. (June 2, 2014), https://www.eff.org/deeplinks/2014/06/top-5-claims-defenders-nsa-have-stop-making-remain-credible [https://perma.cc/37TB-WMYR].

[110] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 11 (2014) https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf [https://perma.cc/8W4L-7EDF].

[111] Schwartz, *supra* note 104.

[112] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 110, at 11.

[113] John Mueller & Mark G. Stewart, *Secret without Reason and Costly without Accomplishment: Questioning the National Security Agency's Metadata Program*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 407, 420 (2014).

expanding the surveillance apparatus necessarily requires a diminishment of resources for traditional and targeted surveillance that, in the past, has proven effective in preventing terrorist attacks.[114]

Beyond material costs, the NSA's bulk telephony metadata program threatens a deep compromise of fundamental civil liberties such as privacy, freedom of speech and association, transparency, due process and the balance of power between the government and its citizens. As a government program, bulk telephony metadata collection must be evaluated not only in light of the ends and values of national security, but also the ends and values of the larger context in which national security is embedded, namely, that of a free, open and above all democratic society. The evidence at hand – costs, benefits, and threats to liberal democratic values – challenges the legitimacy of the bulk telephony metadata collection program.[115]

C. Outlook

The decisions in *ACLU v. Clapper* and *Klayman v. Obama* have both been reviewed by appeals courts. In *ACLU v. Clapper*, the U.S. Court of Appeals for the Second Circuit vacated Judge Pauley's decision, arguing that the bulk telephony metadata program went beyond the statutory authorization of Section 215.[116] In *Klayman v. Obama*, on the other hand, the U.S. Court of Appeals for the D.C. Circuit overruled Judge Leon's injunction on the basis that "the plaintiffs had not met the 'higher burden of proof required for a preliminary injunction' with regard to their standing."[117] Both cases have been remanded to the respective district courts. Meanwhile Congress passed the USA Freedom Act, which, among other things,

---

[114] *See* BERGEN ET AL., *supra* note 104.

[115] For an alternative cost-benefit analysis of the NSA's bulk telephony metadata collection program, see Susan Freiwald, *Nothing to Fear or Nowhere to Hide: Competing Visions of the NSA's 215 Program*, 12 COLO. TECH. L.J. 309 (2014).

[116] ACLU v. Clapper, 785 F.3d 787, 818 (2d Cir. 2015).

[117] Obama v. Klayman, 800 F.3d 559, 564 (D.C. Cir. 2015); *see* Steve Vladeck, *Better Never than Late? The Problematic Standing Holding in Klayman*, JUST SECURITY (Aug. 28, 2015), https://www.justsecurity.org/25665/late-d-c-circuits-problematic-standing-holding-klayman/ [https://perma.cc/6QHZ-XHYE].

prohibits the bulk collection of telephony metadata by the NSA.[118] In future, phone companies rather than the NSA will retain the metadata of their customers.[119] The NSA can access it with court approval. However, neither the passage of the USA Freedom Act, nor the appeals decisions in *ACLU v. Clapper* and *Klayman v. Obama* systematically address the question of how Fourth Amendment challenges to bulk metadata collection programs will be handled in the future – an increasingly important question as the amount and diversity of metadata increases.

IV. CONCLUSION

This paper has demonstrated that a reasonable expectation of privacy depends not only on what metadata *is* – an ontological assessment – but also on the *context* in which it is created and collected – a normative assessment. The paper has shown that the social and technological environment of the NSA's bulk telephony metadata collection program is radically different from that of the pen register collection at issue in *Smith*. These differences primarily manifest themselves in the ability of information subjects to share information *voluntarily*; the ability of the recipients of our metadata to *aggregate*, *store*, *combine* and *analyze* that data; and the extent to which we *assume the risk* of metadata being shared beyond the purpose for which it was originally provided. Significantly, this paper

---

[118] For an overview of the bill, see *USA Freedom Act, H.R. 2048,* U.S. HOUSE OF REPRESENTATIVES JUDICIARY COMM., http://judiciary.house.gov/index.cfm/usa-freedom-act [https://perma.cc/83MX-N4JQ].

[119] Whether this improves the privacy protections of Americans remains to be seen. For instance, the European Court of Justice (ECJ) overruled the EU Data Retention Directive on the basis, among others, that it was unclear whether communications providers could meet "the obligations guaranteeing data protection and security" thus imposed on them. The ECJ further ruled that "the collection and, above all, the retention in huge databases, of the large quantities of data generated or processed in connection with most of the everyday electronic communications of citizens of the Union constitute a serious interference with the privacy of those individuals, even if they only establish the conditions allowing retrospective scrutiny of their personal and professional activities. The collection of such data establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, none the less constitutes a permanent threat throughout the data retention period to the right of citizens of the Union to confidentiality in their private lives. The vague feeling of surveillance created raises very acutely the question of the data retention period." Joined Cases C-293/12 & C-594/12, Digital Rights Ireland v. Minister for Commc'n, 2014 E.C.R., 72, 76 (Dec. 12, 2013) (Opinion of Advocate General Cruz Villalón).

proposes a three-pronged test for evaluating if third-party information sharing is voluntary, namely: First, whether a person *knowingly* shares information with a third party; second, whether a person has an *alternative* not to do so; and third, whether that alternative is *reasonable*. The paper draws on the theory of contextual integrity to analyze how fundamental changes in the social and technological environment have affected the *actors*, *attributes* and *transmission principles* of relevant information flows, and concludes that the NSA's bulk telephony metadata collection program violates the principle of contextual integrity. An evaluation of the program in light of contextually specific values and ends demonstrates that the costs incurred by the collection of telephony metadata in bulk – both in material terms in the context of national security *and* in terms of the fundamental civil liberties affected by the program, such as privacy, freedom of speech and association, transparency, due process and the balance of power between a government and its citizens – call into question the program's moral legitimacy. Most importantly, the paper demonstrates that the main assumption underlying the NSA's program – namely, that metadata, by definition, is non-sensitive data – no longer makes sense. Indeed, according to the theory of contextual integrity, it never made any sense to begin with.